



## UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/724,995	12/01/2003	Nancy Cam Winget	72255/00010	3154
23380	7590	02/01/2007	EXAMINER	
TUCKER, ELLIS & WEST LLP 1150 HUNTINGTON BUILDING 925 EUCLID AVENUE CLEVELAND, OH 44115-1414			POPHAM, JEFFREY D	
		ART UNIT	PAPER NUMBER	
		2137		

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/01/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/724,995	WINGET ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Jeffrey D. Popham	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 01 December 2003.
- 2a) This action is FINAL.                  2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1-23 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 01 December 2003 is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All    b) Some \* c) None of:
1. Certified copies of the priority documents have been received.
  2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date 20050314.
- 4) Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) Notice of Informal Patent Application
- 6) Other: \_\_\_\_\_.

**Remarks**

Claims 1-23 are pending.

***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

1. Claims 22-23 are rejected under 35 U.S.C. 101 because a "computer-readable medium" is defined in the specification as being both physical media and signals. When claims 22-23 are stored on a physical media (e.g. CD-ROM) and executed by a processor, they are statutory, however when they are embodied in a carrier wave, they are not statutory. Clarification of these claims as being on a physical medium and executed by a processor is required.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-6, 9, 10, and 12-21 are rejected under 35 U.S.C. 102(b) as being anticipated by Funk (PAUL FUNK; Simon Blake Wilson; "draft-ietf-pppext-eap-

ttls-02.txt: EAP Tunneled TLS Authentication Protocol (EAP-TTLS)"; Internet-Draft PPPEXT Working Group; 30 Nov. 2002, pp. 1-40).

Regarding Claim 1,

Funk discloses a method of authenticating communication between a first and a second party, the method comprising:  
Provisioning a first secure credential between the first party and the second party (Pages 11-13, sections 6-6.2);  
Establishing a secure tunnel between the first party and the second party using the first secure credential (Pages 11-13, sections 6-6.2);

Authenticating a relationship between the first party and the second party within the secure tunnel using a second secure credential to establish an authorization policy (Pages 11-13, sections 6-6.2); and

Distributing an update to one of the first secure credential and the second secure credential within the secure tunnel to update the authorization policy (Pages 14-15, section 6.4-6.4.1).

Regarding Claim 17,

Claim 17 is a system claim that corresponds to method claim 1 and is rejected for the same reasons.

Regarding Claim 2,

Funk discloses protecting termination of the authenticated communication by use of a tunnel encryption and authentication to

protect against a denial of service by an unauthorized user (Pages 9-15, sections 4.3-6.4).

Regarding Claim 3,

Funk discloses that the step of provisioning occurs within a wired implementation (Pages 4-5, section 2).

Regarding Claim 19,

Claim 19 is a system claim that corresponds to method claim 3 and is rejected for the same reasons.

Regarding Claim 4,

Funk discloses that the step of provisioning occurs within a wireless implementation (Pages 4-5, section 2).

Regarding Claim 18,

Claim 18 is a system claim that corresponds to method claim 4 and is rejected for the same reasons.

Regarding Claim 5,

Funk discloses that the first secure credential is a protected access credential (Pages 11-13, sections 6-6.2).

Regarding Claim 20,

Claim 20 is a system claim that corresponds to method claim 5 and is rejected for the same reasons.

Regarding Claim 6,

Funk discloses that the protected access credential includes a protected access credential key (Pages 11-16, sections 6-7).

Regarding Claim 9,

Funk discloses that the protected access credential includes a protected access credential opaque element (Pages 3-4, section 1; and Pages 10-13, sections 5-6.2).

Regarding Claim 10,

Funk discloses that the protected access credential includes a protected access credential information element (Pages 11-13, sections 6-6.2).

Regarding Claim 12,

Funk discloses that the step of provisioning occurs through in-band mechanisms (Pages 11-13, sections 6-6.2).

Regarding Claim 13,

Funk discloses that the step of establishing the secure tunnel includes the step of establishing a tunnel key using a symmetric cryptographic technique (Pages 11-13, sections 6-6.2).

Regarding Claim 14,

Funk discloses that the step of establishing a tunnel key further includes the step of establishing a session key seed to be used in protecting integrity of the secure tunnel and establishing a master session key (Pages 11-16, sections 6-7).

Regarding Claim 15,

Funk discloses that the step of authenticating is performed using EAP-GTC (Pages 21-22, section 10.2.1).

Regarding Claim 16,

Funk discloses that the step of authenticating is performed using MS-CHAP v2 (Pages 23-24, section 10.2.4).

Regarding Claim 21,

Funk discloses that the wireless network is an 802.11 wireless network (Pages 4-5, section 2).

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 5-11, 20, 22, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Funk in view of Schneier (Schneier, Bruce, "Applied Cryptography", second edition, 1996, pp. 151-157, and 566-571).

Regarding Claim 5,

Funk may not disclose that the first secure credential is a protected access credential.

Schneier, however, discloses that the first secure credential is a protected access credential (Pages 566-571, section 24.5). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the Kerberos

authentication protocol of Schneier into the EAP-TTLS system of Funk in order to provide a trusted party which creates shared secret information used for encryption and decryption between two entities, and to distribute such information to the entities in such a way as to provide authentication of the entities and the trusted party.

Regarding Claim 20,

Claim 20 is a system claim that corresponds to method claim 5 and is rejected for the same reasons.

Regarding Claim 6,

Schneier discloses that the protected access credential includes a protected access credential key (Pages 566-571, section 24.5).

Regarding Claim 7,

Schneier discloses that the protected access credential key is a strong entropy key (Pages 566-571, section 24.5).

Regarding Claim 8,

Funk as modified by Schneier discloses the method of claim 7, in addition, Schneier discloses that the entropy key is a 32-octet key (Pages 151-158, section 7.1). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the key length of Schneier into the EAP-TTLS system of Funk as modified by Schneier in order to provide a strong

symmetric key that is very difficult to break, thus further securing the system.

Regarding Claim 9,

Schneier discloses that the protected access credential includes a protected access credential opaque element (Pages 566-571, section 24.5).

Regarding Claim 10,

Schneier discloses that the protected access credential includes a protected access credential information element (Pages 566-571, section 24.5).

Regarding Claim 11,

Funk does not disclose that the step of provisioning occurs through out-of-band mechanisms.

Schneier, however, discloses that the step of provisioning occurs through out-of-band mechanisms (Pages 566-571, section 24.5). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the Kerberos authentication protocol of Schneier into the EAP-TTLS system of Funk in order to provide a trusted party which creates shared secret information used for encryption and decryption between two entities, and to distribute such information to the entities in such a way as to provide authentication of the entities and the trusted party.

Regarding Claim 22,

Funk discloses an article of manufacture embodied in a computer readable medium for use in a processing system for communicating via a network, the article comprising:

A provisioning logic for causing the processing system to establish a credential between a first party and a second party  
(Pages 11-13, sections 6-6.2);

A tunnel establishment logic for causing the processing system to establish a secure tunnel based upon the credential  
(Pages 11-13, sections 6-6.2);

An authentication logic for causing the processing system to authenticate a communication link between the first and the second party within the secure tunnel based upon a secure credential  
(Pages 11-13, sections 6-6.2);

A second provisioning logic for causing the processing system to provision an access (Abstract; Pages 5-8, section 3; and Pages 11-13, sections 6-6.2); and

A delivery logic for causing the processing system to deliver an update to one of the credential and the secure credential via the network (Pages 14-15, section 6.4-6.4.1);

But does not explicitly disclose that the credential is a shared secret.

Schneier, however, discloses that the credential is a shared secret (Pages 566-571, section 24.5). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the Kerberos authentication protocol of Schneier into the EAP-TTLS system of Funk in order to provide a trusted party which creates shared secret information used for encryption and decryption between two entities, and to distribute such information to the entities in such a way as to provide authentication of the entities and the trusted party.

Regarding Claim 23,

Funk as modified by Schneier discloses the article of manufacture of claim 22, in addition, Funk discloses that the tunnel establishment logic further includes a key generation logic for causing the processing system to generate a secure key for encrypting and signing a communication between the first party and the second party (Pages 11-16, sections 6-7; and Pages 36-37, section 14).

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

Art Unit: 2137

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham  
Examiner  
Art Unit 2137

  
EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER